TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

HACKER JOURNAL

INTERNET & CENSURA

LA LIBERTÀ È COSÌ SCONTATA?

2€
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

CARTA DI CREDITO

ECCO I PERICOLI CHE CORRIAMO

PEER TO PEER

Tutti i segreti SVELATI!

NUOVI GIOCHI SU N-GAGE

CRITTOGRAFIA A PROVA DI BOMBA

QUATTORDICINALE

4ever



Anno 3 – N. 64
2/16 Dicembre 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."



editoriale

NOI Siamo DIVERSI

Sono stato a Milano alla presentazione dell'ultimo libro di Donald Norman. Si chiama Emotional Design e viene pubblicato in edizione italiana da Apogeo. Chi è Donald Norman? Che domande. Un hacker. Come, un hacker? Ma dove è entrato? Che siti ha defacciato? In che linguaggio scrive i suoi programmi?

No. Donald Norman è un hacker. Solo che lui, invece di occuparsi di computer o di reti, si occupa di come si progettano le cose (anche i computer). Il suo primo libro si chiamava, in italiano, La caffettiera del masochista. Qualcuno ricorderà la copertina. Una teiera con il manico messo dalla stessa parte del beccuccio. Impossibile versare il tè senza rovesciarselo addosso.

Chi progettasse una teiera del genere sarebbe giudicato imbecille. Ma nella tecnologia agiscono indisturbati centinaia, migliaia di imbecilli che progettano e programmano sistemi imbecilli come loro. Sono quelli che hanno inventato il messaggio di errore Tastiera non trovata. Premere F1 per continuare. Chi ha stabilito che bisogna riavviare il computer per cambiare la risoluzione dello schermo è un imbecille. Chi fa i portatili con la trackpad spostata a sinistra è un imbecille. A meno che volesse vendere computer solo ai mancini. Mettere la trackpad in mezzo è possibile. Un sacco di portatili ce l'ha in mezzo. Chi la vende spostata a sinistra è imbecille quasi come chi la compra e poi si lamenta che gli fa male il polso.



Norman è un hacker perché smaschera l'imbecillità dei progettisti e insegna a tutti come devono essere fatte le cose. Che devono essere al nostro servizio e non il contrario. Ecco perché è hacker. Quando ti installano in casa il contatore digitale, che non ti lascia usare gli stessi elettrodomestici che usai prima perché è male programmato, lì serve un hacker. Quando si crea un browser bacato come Explorer, gli hacker scrivono Firefox, che è migliore. Fanno la stessa cosa che fa Norman con le teiere, o i videoregistratori.

Alla conferenza stampa di Norman c'ero anch'io. Avevo una maglietta con la scritta Hacker Journal. Mi ha visto un altro ragazzo. "Complimenti per la maglietta… ma tu scrivi su Hacker Journal?", mi ha chiesto.

Ho sorriso. "No", ho risposto, "ma conosco quelli che lo fanno…"
A fare Hacker Journal siamo tutti noi, che scriviamo, che leggiamo, che ascoltiamo. Quelli diversi. Quelli curiosi. Con la voglia di imparare. Hacker.

theguilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo… Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea: Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron Simone Tarantino, Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo
Elenina "menosina" Varesi

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Distributore per l'estero:
Johnsons International News Italia Spa
Via Valparaiso, 4
20144 Milano - Italia

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15 - Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

NET? NIET!

Dalla Russia giungono voci governative che auspicano la censura di Internet. La libertà che abbiamo è davvero così scontata? Si comincia il 15 novembre, con Andrey Fursenko, Ministro per l'Istruzione e la Scienza della Federazione Russa. Fursenko interviene durante il Forum scientifico mondiale di Kyoto e sostiene di volere il controllo statale di Internet nel suo Paese.

Si prosegue con Sergei Lavrov, Ministro degli Esteri del gabinetto di Putin, il quale secondo l'agenzia di stampa Novosti definisce inaccettabile che i siti Internet non possano essere controllati.

nel caso specifico limitando pesantemente il raggio d'azione della versione cinese del più noto motore di ricerca al mondo. L'alternativa? Restare fuori. Dopotutto anche quello cinese è un mercato e in numeri in ballo, in un futuro, sono belli grossi. Nel Medio Oriente, dall'Iran in poi, sono numerose le nazioni dove la Rete è fortemente regolamentata, censurata oppure punita al punto che i pochi cybercafè esistenti sono sempre sul filo della chiusura d'autorità. In Vietnam il regime si è aperto al libero mercato, ma Internet è sempre ostacolata in tutti i modi. Non parliamo di Paesi come Corea del Nord o Cuba.

PICCOLA AZIONE PER UNA GRANDE CAUSA

Sulla pagina http://www.eff.org/br/ ci sono tutte le istruzioni per partecipare alla campagna Blue Ribbon della Electronic Frontier Foundation. Un nastro blu da mettere nei nostri siti per fare sapere che siamo a favore della libertà di parola e di informazione. E come potrebbe essere diversamente, se siamo hacker?

```
<BR /><DIV ALIGN="CENTER">
<A HREF="http://www.eff.org/br/">
<IMG SRC="http://www.eff.org/br/br.gif"
ALT="Join the Blue Ribbon Online Free
Speech Campaign"
HEIGHT="76" WIDTH="112" BORDER="1"
ALIGN="MIDDLE">
<BR />
Join the Blue Ribbon Online Free Speech
Campaign!</A>
</DIV>
<BR />
```



LA FINE DI LIN

Lin Hai è un cinese esperto di computer. Viveva a Shanghai, ma ha dovuto trasferirsi negli Stati Uniti, dopo avere scontato un anno e mezzo di galera nelle prigioni della Cina. La sua colpa? Avere passato indirizzi email "proibiti" a una rivista online dissidente.
Come lui ce ne sono migliaia e forse più. Non dimentichiamocene.

Questa è la stretta attualità. Ma da tempo ci sono nel mondo situazioni croniche di censura o limitazione pesante di Internet.

A Singapore vige uno stretto controllo della Rete e vengono applicate sanzioni molto severe nei confronti di chi sgarra. In Cina l'accesso viene enormemente limitato. Su oltre un miliardo di persone meno di un decimo ha il collegamento. La consultazione di siti proibiti è punita dalla legge e comunque il governo fa del suo meglio per bloccare al confine i siti che reputa pericolosi. Colossi come Google hanno dovuto prendere la strada del compromesso,

Per paradosso, sono proprio le nazioni più severe nei confronti di Internet quelle da cui provengono contenuti Web su cui più di una persona ragionevole avrebbe qualcosa da obiettare. In Russia risiede una quantità abnorme di siti dedicati alla pedopornografia e in generale alla pornografia minorile. Sono cinesi moltissimi siti di duplicazione abusiva di software (e qui non si parla di warez, ma di vera e propria pirateria commerciale). In Medio Oriente abbondano i siti che appoggiano il terrorismo, quando non pubblicano video e fotografie di decapitazioni ed esecuzioni varie.

Quasi quasi, a pensarci, in Occidente abbiamo i nostri problemi con i contenuti Internet. Ma per una pagina pornografica o di odio razziale ne abbiamo numerose altre, valide, istruttive e interessanti in tutti i campi.

Non sarà che il modo migliore per controllare Internet è lasciarla libera, esattamente come il telefono o il fax, e lasciare che le persone normali e sensate mettano in minoranza pervertiti, assassini e truffatori, come è normale? Camminando per la strada possiamo incontrare una persona cattiva. Ma ce ne sono centinaia buone. Internet non è diversa.

Barg the Gnoll
gnoll@hackerjournal.it

NEWS



PENTIUM OLTRE I 6 GHZ!



Abbiamo già parlato del raffreddamento di un Pentium 4 con l'azoto liquido, per cercare nuove strade all'overclocking. Ma la sfida non è finita: un gruppo tedesco è riuscito a far girare un Pentium 4 alla bellezza di 6,3 Ghz raffreddandolo con un sistema a tre stadi che utilizza gas non nocivi. Fino a prova contraria lo si può incoronare come il sistema migliore finora costruito. Complimentoni! Tutte le info e le foto all'indirizzo: www.hardwareluxx.de

ADSL A 12 MEGA DA TISCALI?

tiscali.broadband

Benvenuto nel mondo della SuperVelocità!

12 mega — Adsl Flat — L'Adsl più veloce in Italia — 99.95 € mese anziché 149.95 — 99.95 €/mese invece che 149.95 €, per sempre, se attivi entro il 25 novembre 2004 — VAI

6 mega — Adsl Flat — Tuffati nel mondo dell'alta velocità — 69.95 € mese anziché 99.95 — 69.95 €/mese invece che 99.95 €, per sempre, se attivi entro il 25 novembre 2004 — VAI

Quasi 150 euro al mese, ma Tiscali promette una Adsl a 12 Mbps che diventerebbe la più veloce d'Italia.
Peccato che inserendo qualunque numero di telefono di tante zone d'Italia diverse, anche di grandi città, siamo stati riportati sempre alla pagina dei 640 Kbps o a una pagina che ci avverte che la zona non è coperta (da cosa, da Adsl? Ma se già l'abbiamo!...). Con un messaggio che promette di tenerci informati, compilando un apposito form, se e quando saremo raggiunti dalla nuova linea. Probabilmente, per ora, un metodo per sapere se c'è un reale interesse per un'offerta di alte prestazioni, ma anche di costo elevatissimo. Sarebbe utile conoscere anche la banda garantita, dovendo spendere non pochi soldi al mese.

IL PRIMO GIORNO DI HALO-2

Vendite per 100 milioni di dollari il primo giorno di Halo-2, il nuovissimo titolo di Microsoft per X-Box. Nella foto, la folla in attesa fin dalla notte precedente in Times Square, a New York, l'8 novembre 2004.



CINQUE ANNI AL TRUFFATORE

È australiano e dal suo paese spediva a utenti in tutto il mondo (chi non l'ha mai ricevuta alzi la mano) un'email di un improbabile personaggio nigeriano che chiedeva di trasferire del denaro su un conto europeo, promettendo ricompense da favola. Naturalmente, prima, riusciva con un complicato raggiro a farsi versare notevoli quantità di denaro da quelli che ci cascavano. Così ha raggranellato nel frattempo 3 milioni di euro, ma è stato beccato, imprigionato e finalmente non potrà fare danno per i prossimi cinque anni. Morale: qualunque email riceviate che non sia della vostra fidanzata, buttatela. Soprattutto se vi chiede soldi.

NUOVO WORM PER EXPLORER

Sfrutta la vulnerabilità di IFRAME, all'interno di Microsoft Explorer. Si chiama W32/Bofra ed esiste in tre varianti: A, B e C. Tutte e tre si beccano seguendo le istruzioni di una falsa comunicazione che sembra arrivare da PayPal, ma ci inganna chiedendoci un semplice click su un link sconosciuto. Da lì arriva sul nostro pc un bel worm che si diffonde replicandosi a tutti gli indirizzi di email della nostra rubrica di Outlook. Insomma, l'ennesimo problema per chi usa il sistema operativo Microsoft. Niente di nuovo sotto il sole, ma sempre pericoloso.

IBM, IL PIÙ VELOCE

Se stiamo pensando di raddoppiare il nostro Pentium per avere una macchina più veloce, non scoraggiamoci. Siamo sulla buona strada per raggiungere i 16 mila processori che Ibm ha messo in fila per costruire il più veloce computer del mondo. E' capace di 70 mila









MOZILLA CONTRO EXPLORER



È disponibile la versione 1.0 di Firefox, il browser Mozilla che sfida a tutto campo la pesantezza di Microsoft Explorer. Più veloce nella costruzione delle pagine, inattaccabile perché senza vistose falle alla sicurezza, più leggero perfino di Opera. In soli 4,5 Mbyte sono riusciti a comprimere tutte le funzionalità che si vorrebbero da un browser. Peccato che in queste ore sia sempre più difficile scaricarlo dal sito: la corsa al download sta mettendo a dura prova perfino i server di Mozilla Foundation, all'indirizzo www.mozilla.org.

MEMORIZZA LA SCRITTURA

Lo applichiamo in cima a un blocco di fogli, come una pinza. Lui ci investe di un fascio di raggi infrarossi e capisce dove e cosa stiamo scrivendo. Traduce in Ascii e il gioco è fatto: abbiamo digitalizzato la scrittura manuale. Beh, forse non sono tutte rose e fiori, anzi numeri e lettere, ma la sostanza è questa. Provare a guardare www.nexconcepts.com



DISPLAY CILINDRICO

Sviluppato in Giappone, è un display a 91" visibile da tutte le angolazioni, anche da dietro. Com'è possibile? Semplicemente perché è cilindrico e srotola qualunque immagine, o qualunque filmato, su tutta la superficie. Un po' scomodo correre in continuazione in tondo per capire chi sta sparando al nostro attore preferito durante la visione del nostro film preferito, ma tant'è.



La soddisfazione è massima quando lo vedranno i nostri amici e ci chiederanno quanto l'abbiamo pagato. Potremo dire loro di essere tra i pochi ad avere in casa un oggettino da 93 mila dollari (sì, abbiamo scritto giusto).

MOTORE DI RICERCA PER P2P

Alla faccia di tutte le leggi contro il p2p, all'indirizzo http://yotoshi.com/ è utilizzabile "the bitorrent file search engine" il cui nome già dice tutto. Due menu a tendina aiutano a cercare velocemente file bitorrent o immagini iso, ma anche immagini, documenti, software, audio e video. Di tutto per farsi una copia, naturalmente di backup!, di ogni cosa passi per la testa. Stando attenti a non giocarsela.

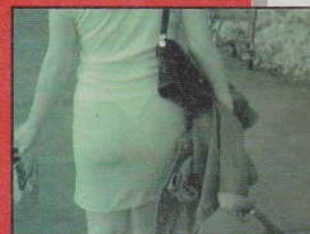


miliardi di operazioni in virgola mobile ogni secondo.

Si chiama Blue Gene/L e sarà installato presso l'Agenzia Nazionale per la Sicurezza Nucleare del Dipartimento dell'Energia americano, innanzitutto per simulare l'utilizzo di armi nucleari, evitando così i test nel sottosuolo. In prospettiva speriamo in qualche utilizzo più pacifico. E da noi? Ecco MareNostrum, il computer spagnolo basato su Linux, sempre di Ibm, che si colloca al quarto posto dei computer più potenti del mondo e al primo in Europa. Ma nel 2005 già ci aspettiamo un salto di qualità: pare che Ibm annunci un computer da 300 mila miliardi di operazioni al secondo. Roba da sballo.

VEDERE ATTRAVERSO I VESTITI...

Qualcuno ha mai visto gli occhiali che promettono di vedere attraverso i muri e sotto le gonne delle signore? Per anni sono stati lo specchietto per le allodole dei creduloni. Ora esiste una versione super tecnologica, pubblicizzata al sito www.advanced-intelligence.com/. Ancora roba da creduloni? Questo è tutto da verificare. Perché la tecnologia esiste ed è quella degli amplificatori di infrarossi. Ogni corpo emette infrarossi e rilevarli con l'aiuto della tecnologia delle macchine fotografiche digitali comporta vedere un esatto profilo del corpo che li emette. E di corpi si tratta anche nelle fotografie di esempio presenti sul sito...

Il blog di DarkSquall''88



Volevo comunicarvi il mio indirizzo di blog dopo aver riletto x 2 o 3 volte l'articolo a pag 8 di non so quale num. (skerzo...). Cmq bando alle ciance e eccovi l'indirizzo del blog: http://darksquall1988.blog.tiscali.it
...e se passate lasciate un commento...grazie...
Un ciao a tutta la vostra crew...! Continuate così!

DarkSquall"88

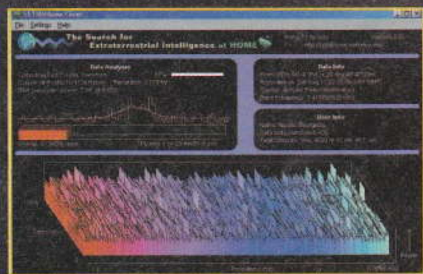
Eccoti accontentato. Mi raccomando, rendilo sempre più bello e interessante da leggere! Altrimenti si fa in fretta, a perdere ammiratori!

Lui è il creatore n°1

Ciao!
Ho creato il Team Hacker Journal per il progetto SETI@home che sfrutta l'interfaccia BOINC. Ci si può iscrivere su http://setiweb.ssl.berkeley.edu, nella sezione "teams". Iscrivetevi, mi raccomando!

Tom182

Bravo! Siamo tutti con te. Ovviamente non sei l'unico...



E lui il creatore n°1

Carissimi di Hacker Journal,
quando ho letto l'articolo sui progetti @HOME mi sono subito "gettato" in rete per aderire al progetto SETI e a quello sulla cura del cancro; a proposito di quest'ultima, ho fondato il team: HJ - SpellBreakers Vi prego di pubblicarmi e invito tutti ad accorrere numerosi! Siete mitici, continuate così!!!

SpellBreaker

Ottimo! Facciamoli vincere, questi team!

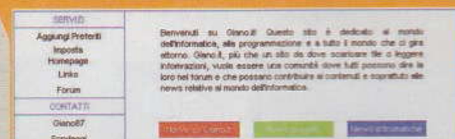


UN ALTRO SITO

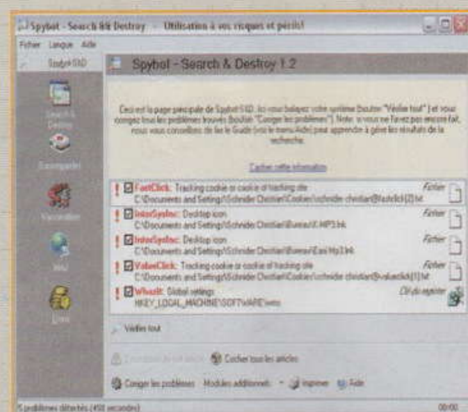
Volevo anche segnalarvi il mio sito (se potete pubblicate almeno questo.. grazie...) : http://gianoit.altervista.org

Giano87

Per le tante domande... alla prossima! Per il sito: eccoti accontentato! Se riuscirai a renderlo ancora più ricco e correggerai i refusi, sarà sicuramente più visitato! Ciao!



Consiglio prezioso



Volevo dare un consiglio ai lettori di hackerjournal, per quanto riguarda la rimozione dei programmi spia, è meglio effettuare la scansione con ad-aware o spybot o di entrambi, quando windows è in modalità provvisoria, questo per evitare che il processo attivo del programma spia reimposti il tutto com'era prima alla fine della scansione.

net_csharp

È giusto. Non l'abbiamo mai sottolineato abbastanza e pensiamo che ad alcuni lettori possa effettivamente risolvere qualche problema! Grazie!

Basta, passo a Linux!

Avevate ragione... Il pinguino linux è contagioso. Grazie per avermi fatto "disintossicare" dall'uso delle finestre.
Mi ero avvicinato da un po di tempo all'Open Source, tramite open office, ma linux è davvero un altro pianeta! Adesso, dopo averlo provato con la distro Knoppix - live, sto aspettando l'uscita di una versione permanent, che sancirà il mio ingresso anche nella comunità dei linux user's. Continuate così e complimenti per la rivista.

Orinoco

W Linux!. Perfino nei supercomputer, quelli che usano 'cubi' di centinaia di processori ciascuno, è installato Linux.
L'ultimo esempio in Spagna: il supercomputer più potente d'Europa, europeo, è basato su Linux.



SETI: IO L'AVEVO GIÀ FATTO

In base a quanto letto nell'ultimo numero di hj , vorrei segnalare il nostro sito, come un collaboratore al progetto "Seti@Home"... oltre ad occuparsi di altri argomenti, molto interessanti : il sito è: www.branzilla.org
Grazie e a presto

.: Branzilla :.

Menzione all'ottimo sito, più che al progetto! Noi vorremmo progetti HJ! :)



APPLE SBAGLIA(VA)

Ovviamente l'indicazione che la calcolatrice di MacOSX 10.3 può produrre qualche problema ha suscitato non poche e interessanti risposte. Per esempio quelle di Gianni Arcieri, ilconte100@fastwebnet.it, MP. Tutti ci dimostrano che non è vero o che abbiamo trattato la cosa superficialmente. Ripetiamo quanto dice Apple stessa. La nota tecnica è all'indirizzo: http://docs.info.apple .com /article.html?artnum=25687. È possibile che nelle versioni superiori a MacOSX 10.3 abbiano posto rimedio, ma abbiamo fatto una prova con una versione 10.3.5 e l'errore è ancora lì.

A caccia di idee

Salve gentile redazione di hj, la vostra rivista è magnifica. Però volavo proporvi una cosa: perchè non mettete una rubrica per gli annunci? Io per esempio ne avrei uno: sono un neo-programmatore in C++. Solo che non ho spunti per realizzare qualcke programmino sfizioso.
Qualcuno può mandarmi qualche idea all'indirizzo reodark@virglio.it? Però non qualcosa di astronomico perke sono alle prime armi. Manderò una copia dei codici a coloro che mi risponderanno. Grazie mille e...W l'open source, abbasso Microsoft, e al diavolo i lamers.

reodark@virgilio.it

Beh, di idee crediamo sia pieno il mondo, a pensarci bene. Perché non cominci da qualcosa che possa servire a te? :)

Div. thm. proof idea (8)

Note complete analogy w/ arguments for fund. thm. of calc I, fund. thm. of line ints, Green's theorem ......

$$\oiint_S \vec{F}\cdot d\vec{S} = \sum_K \oiint_{S_K} \vec{F}\cdot d\vec{S}$$

(defn. of differentiable, locally almost linear; error as small as desired via choice of fine-ness of partition)

$$\approx \sum_K \oiint_{S_K} \vec{L}_K \cdot d\vec{S}$$

(easy proof for linear objects)

$$= \sum_K (\text{trace } L_K)\,\Delta V$$

(defn. of div)

$$\approx \sum_K \iiint_{R_K} (\text{div } F)\,dV$$

(+ defn. of $\iiint$ as limit of R-sums)

$$= \iiint_R (\text{div } F)\,dV$$

Luci Usb grandi o piccole?

EXPECT MORE... GET MORE... FROM DUCOHM — CARBON COMPOSITION INSULATED RESISTORS

DUCON CONDENSER PTY. LTD.

Ciao a tutti, sono il duca, salto i complimenti xkè ho poco tempo... vi scrivo per due problemini... il primo: le resistenze da usare per seguire l'articolo "Hack di un USB" devono essere quelle "grandi" o quelle "piccole"? il secondo: ho registrato il mio nick su IRC e adesso non mi fa più accedere con esso! a proposito, xkè non fate un pò più articoli sull'elettronica? x il resto continuate così... Ciao.

Il Duca

Se è perché non hai tempo, figurati noi! :)
Risposta a): quelle piccole. Le potenze in gioco sono minime.
Risposta b): boh!
Risposta c): perché mancava la tue email per farci decidere! ;)

DVD NON ECOLOGICI?

Ciao, leggendo la news sui DVD usa e getta, mi è venuta spontanea una domanda; dopo aver passato anni a convincerci che l'usa e getta è sbagliato perché si inquina a più non posso, perché si incoraggia lo spreco di risorse ecc., per di più in un epoca in cui i contenuti si possono trasmettere via internet senza praticamente alcuno spreco (tranne un po' di elettricità), ecco che appare l'uovo di Colombo, il DVD usa e getta. Ma le tonnellate di DVD prodotte con questo sistema che fine faranno? Si potrà almeno riciclarle oppure entreranno a far parte di quella grossa fetta di rifiuti che l'era informatica sembrava dover eliminare?

Ubique

Bella domanda. E noi lettori, cosa pensiamo sull'argomento?



È sufficiente aprire un'immagine .png per essere colpiti e affondati: in un mare di dati di un attacco buffer-overflow

L'IMMAGINE

La compressione .png è una delle migliori compressioni possibili da applicare a un file d'immagine da inviare sulla rete, perché è efficiente e non comporta nessuna perdita di dati. Costruire un sistema di compressione e visualizzazione delle immagini non è roba da poco. Oltre a pensarlo con delle caratteristiche specifiche, adatte alla trasmissione di immagini sulla rete, bisogna creargli un contorno di librerie: dei pezzi di software che permettono agli sviluppatori delle applicazioni che ne fanno uso di incorporarlo e di farlo funzionare. Per il formato .png le librerie principali create e mantenute aggiornate sono due: zlib e libpng. La prima si occupa della compressione, la seconda di tutto il resto. Libpng è il frutto di un progetto OpenSource nato fin dal 1995. Tutti i programmatori che scrivono delle applicazioni che usano il formato png devono fare uso delle funzioni di libpng inglobandole nel loro codice.

Le vulnerabilità

Attenzione alla versione, però. Perché nelle versioni precedenti la 1.2.7 sono state scoperte delle vulnerabilità non da poco. Qualunque applicazione faccia uso di libpng in versioni precedenti la 1.2.7 è seriamente minacciabile semplicemente scaricando un'immagine .png. Al punto che l'attaccante può prendere il controllo dell'applicazione stessa, facendo eseguire apposito codice inserito nel formato dei dati png. Un guaio serio, di cui ci si è accorti solamente nel mese di agosto di quest'anno.
Un'immagine .png contiene obbligatoriamente dei pezzi di software che si chiamano IHDR, IDAT e IEND. Oltre a questi, nelle specifiche dello standard png è permesso che l'immagine possa contenere altri pezzi di codice. Per esempio il codice opzionale tRNS è quello che nelle immagini gestisce la caratteristica di trasparenza. All'interno del pezzo tRNS ci sono diversi blocchi di codice, che possono essere manipolati da un attaccante. Se si omette il blocco PLTE, si crea una condizione per un errore logico che produce un buffer overflow. La funzione che crea il problema è la png_handle_tRNS(), che ha la responsabilità di assicurare la corretta formattazione delle immagini png. Quando si trattano delle immagini png non create correttamente o alterate, questa funzione può miseramente cadere sulla corretta autenticazione della lunghezza dei dati relativi ai pezzi in trasparenza. Le applicazioni che supportano il formato .png possono essere parecchie: dai navigatori ai programmi di posta elettronica, alle diverse utility grafiche. Tutte le applicazioni che utilizzano la libreria libpng potrebbero quindi essere toccate dal problema.

Le soluzioni

Una patch della patch. Perché la libreria libpng è stata corretta, ma introducendo un banale errore di programmazione: sbagliava l'intestazione del formato dei file. Quindi è stata rilasciata un'altra patch, finalmente definitiva, che è la 1.2.7. Già, ma nel frattempo? Siamo al sicuro quando utilizziamo, per esempio, Word o Explorer? Ovviamente no, se non abbiamo scaricato gli aggiornamenti di Office dal sito Microsoft.
Così anche per MacOSX esiste l'aggiornamento che mette al riparo dalle bizze del formato png. Lo troviamo all'indirizzo www.download.com/Apple-Security-Update-for-Mac-OS-X-10-3-4/3000-2283-10315112.html
Oppure consultiamo il documento all'indirizzo http://docs.info.apple.com/article.html?artnum=25791 e facciamo così un aggiornamento globale che comprende anche tutte le patch di sicurezza fino a ora uscite per i sistemi Apple.



ASSASSINA

ATTENZIONE ALLA PRONUNCIA

I suoi creatori dicono che la pronuncia esatta è ping, che poi sarebbe l'acronimo di Portable Network Graphics, ma anche di PiNG is Not Gif, perché il formato png è nato quasi come una sfida al GIF, usato inizialmente da Compuserve e fino a poco

.PNG vs .GIF

tempo fa coperto da brevetto (a proposito: pronunciamo Gif con la G dolce come giraffa o Gif con la G dura come gatto? Risposta esatta: G dolce)



Open Source non vuol dire assenza d'errori, ma una comunità che lavora per correggerli

NON UNA, TANTE

La vulnerabilità di libpng di cui abbiamo detto è la più pericolosa. Ma la realtà è peggiore. Sono state scoperte diverse vulnerabilità nella stessa libreria:

- il puntatore libpng png_handle_iCCP() NULL non porta a nulla durante un'operazione di allocazione della memoria.
- si ha un libpng integer overflow quando libpng fa uso della funzione png_read_png()
- la funzione libpng png_handle_sPLT() può portare in overflow durante le operazioni di allocazione della memoria.
- libpng png_handle_sBIT() esegue dei controlli insufficienti di limite della memoria.

NEL BAZAR

Esploriamo i segreti delle reti p2p più frequentate e dei

Milioni di utenti in tutto il mondo si scambiano file d'ogni tipo collegando i loro computer tramite le reti peer-to-peer. Le associazioni delle case discografiche e dei produttori video ci mentono spudoratamente: non è vero che più avanza la lotta alla pirateria e meno utilizzate sono le reti p2p. Stando ai numeri, gli utenti p2p sono in continua crescita in tutto il mondo, chi su una rete, chi su un'altra. Ma diamo un'occhiata ai sistemi principali, che funzionano come niente fosse sotto lo sguardo terrorizzato di chi vorrebbe controllare tutto e limitare la libertà di Internet.
Tutti i programmi indicati esistono in diverse versioni per sistemi operativi differenti, quasi tutti sono disponibili per Linux, MacOS e Windows. Diamo le indicazioni per scaricare la versione Windows, ma dal sito principale è facile trovare le altre.

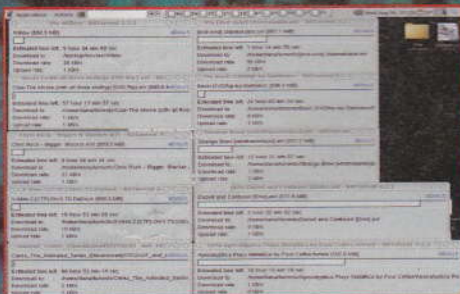
LE LIMITAZIONI DI SP2

Il Service Pack2 di Windows, SP2, e le sue sicurezze crea non pochi problemi ad alcuni programmi p2p, come eMule , BitTorrent, SoulSeek e altri. Perché limita le connessioni TCP contemporanee. È possibile rimediare intervenendo sui file di registro andando a cambiare il valore di una variabile che si chiama DWORD e che si raggiunge così:

System Key: [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]
Value Name: TcpNumConnections
Data Type: REG_DWORD (DWORD Value)
Value Data: 0 - 0xfffffe

BITTORRENT

È un sistema p2p che consente di trasferire file molto grandi contemporaneamente a molti utenti. Quando usiamo BitTorrent in realtà non facciamo nessuna ricerca di file presso altri utenti, come nel normale p2p. Invece raggiungiamo un server centrale dove c'è una lista di tutti i più recenti trasferimenti di file. Le liste di server che tengono traccia dei file trasferiti e di dove andarli a cercare, costituiscono i file .torrent che sono innanzitutto scaricati dal client. Dopodiché è interrogato il server che li indirizza e quindi viene caricato il file da dove fisicamente si trova.



BITTORRENT
VERSIONE CORRENTE: 3.4.2
RILASCIATA: aprile 2004
INDIRIZZO DI DOWNLOAD: http://bittorrent.com/download.html
DIMENSIONE FILE: 2.226 KB
HOMEPAGE: http://bittorrent.com/

FASTTRACK

La rete FastTrack è la rete del popolare programma Kazaa, Grokster e iMesh. È una rete decentralizzata, che significa che non esiste un nodo centrale di smistamento, ma ogni computer è collegato direttamente a un altro. Ha però la caratteristica di creare dei server temporanei di indicizzazione degli utenti su una qualunque macchina abbastanza potente che trovi collegata. Quindi anche noi potremmo diventare un temporaneo server, che facilita la ricerca spezzando in sottoreti l'enorme massa di utenti che accedono normalmente con Kazaa. La stabilità del tutto ha portato FastTrack a essere utilizzata da oltre 4 milioni di utenti.



KAZAA
VERSIONE CORRENTE: 2.6.6 (italiano), 2.7 (inglese)
RILASCIATA: aprile 2004
INDIRIZZO DI DOWNLOAD: www.kazaa.com/it/products/downloadKMD.htm
DIMENSIONE FILE: 6,7 MB
HOMEPAGE: www.kazaa.com




DEL P2P

programmi che ne fanno uso!

TROVIAMO I PROGRAMMI DI CUI SI PARLA IN QUESTO ARTICOLO SU HACKERS MAGAZINE NUMERO 25



BITTORNADO

VERSIONE CORRENTE:
T-0.3.8
RILASCIATA:
ottobre 2004
INDIRIZZO DI DOWNLOAD:
http://www.bittornado.com/download.html
DIMENSIONE FILE: 3,56 MB
HOMEPAGE: http://bittornado.com/````

BITCOMET

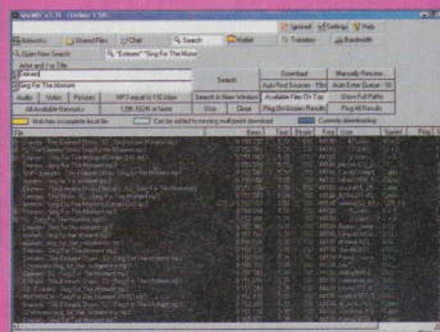
VERSIONE CORRENTE: 0.56
RILASCIATA:
ettembre 2004
INDIRIZZO DI DOWNLOAD:
www.bitcomet.com/doc/download.htm
DIMENSIONE FILE: 1,649 KB
HOMEPAGE: www.bitcomet.com

OPENNAP E WPNP

Nell'era di Napster, WinMX era un client apprezzato e utilizzato da un numero impressionante di utenti. Qualche anno fa la rete di Napster, OpenNap, venne però accusata di facilitare il traffico illecito di file musicali mp3. Con l'azione legale della potente associazione delle case discografiche americane, RIAA, ha quindi subito un colpo mortale e ne è seguito un periodo di caos. Fino al rilascio della versione 2,5 di WinMX. Oltre a mantenere il supporto della defunta rete OpenNap, WinMX ha introdotto il protocollo di rete WPNP (WinMX Peer Networking Protocol). Così facendo, a fronte di un semplice aggiornamento della versione, gli oltre 100 mila utenti dell'era di Napster si sono tro-

WINMX

VERSIONE CORRENTE: 3.53
RILASCIATA: luglio 2004
INDIRIZZO DI DOWNLOAD:
http://dld91.winmx.com/8198751285/winmx353.exe
DIMENSIONE FILE: 804 KB
HOMEPAGE: www.winmx.com







IMESH

VERSIONE CORRENTE:
4.5 build 150
RILASCIATA: febbraio 2004
INDIRIZZO DI DOWNLOAD:
www.imesh.com/download/download.php
DIMENSIONE FILE: 3.16 MB
HOMEPAGE: www.imesh.com

GROKSTER

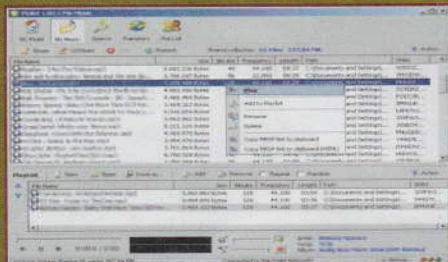
VERSIONE CORRENTE: 2.6
RILASCIATA: febbraio 2004
INDIRIZZO DI DOWNLOAD:
http://www.download.com/Grokster/3000-2166-10237041.html?part=dl-grokster&subj=dl&tag=button
DIMENSIONE FILE: 251.27 KB
HOMEPAGE: www.grokster.com

Manolito P2P network

Pura musica. Solamente MP3. Niente video, .torrent, Dvd o chissà cos'altro. La rete Manolito è dedicata solamente allo scambio di file MP3 ed è anche molto controllata. Praticamente inesistenti file incompleti o corrotti. È nata nel 2001 in Spagna per opera di un unico programmatore: Pablo Soto. Come FastTrack, WinMX o Gnutella anche Manolito è una rete senza server centrale e quindi più resistente agli attacchi legali della potente associazione delle case discografiche americane.

PIOLET

VERSIONE CORRENTE: 2.0
RILASCIATA: marzo 2003
INDIRIZZO DI DOWNLOAD: www.piolet.com/download/
DIMENSIONE FILE: 504.36 KB
HOMEPAGE: www.piolet.com/

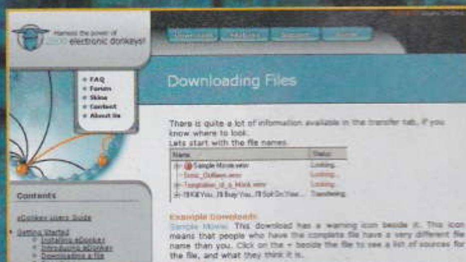


eDonkey2000

È una rete centralizzata, quindi utilizza un server a cui tutti i client fanno riferimento. Ovviamente così facendo è sottoposta agli attacchi della RIAA e di chi vuole limitare lo scambio di file p2p. Per lo stesso concetto aveva dovuto chiudere Napster, che era una rete centralizzata in California. Per cercare di evitare problemi di questo tipo eDonkey non adotta un unico server centrale, ma ce ne sono diversi e non hanno mai un'unica collocazione precisa. Si è sempre distinta come la rete per le risorse di video, film, immagini ISO di CD, e gli album completi. Roba pesante, insomma. Così facendo si pone come alternativa ai Newsgroup più spinti o alle reti IRC. Pare che attualmente comprenda oltre 1 milione di utenti.
Ora comprende anche la rete OverNet e la nuova versione di eDonkey può usare entrambe le reti. OverNet è nata come rete decentralizzata, alternativa a eDonkey2000. Ma quest'ultima non è mai morta anche grazie alla diffusione di eMule, uno dei client che ne fa uso.

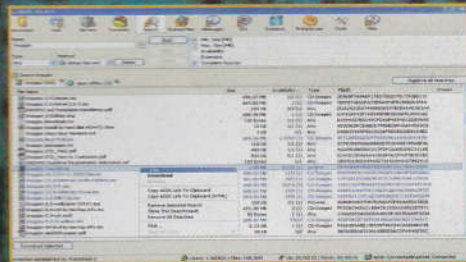
EMULE

VERSIONE CORRENTE: 0.44d
RILASCIATA: novembre 2004
INDIRIZZO DI DOWNLOAD: http://www.emule-project.net/home/perl/general.cgi?l=1&rm=download
DIMENSIONE FILE: 4.058 KB
HOMEPAGE: www.emule-project.net



EDONKEY

VERSIONE CORRENTE: 1.0
RILASCIATA: agosto 2004
INDIRIZZO DI DOWNLOAD: www.edonkey2000.com/downloads.php
DIMENSIONE FILE: 2,36 MB
HOMEPAGE: www.edonkey2000.com oppure www.overnet.com



Gnutella

Una rete decentralizzata, quindi senza server localizzati da qualche parte. Invece, anche il nostro pc può diventare di supporto alla rete Gnutella, se viene "promosso" a nodo super-peer, capace di tenere indicizzati degli indirizzi di altri client e quindi aiutando a spezzare la rete globale in sottoreti più ridotte e più facilmente consultabili.Inizialmente è stata sviluppata da Justin Frankle di NullSoft. Con il programma Shareaza è stata sviluppata una versione chiamata Gnutella 2 che ha risolto alcuni possibili problemi di sovraccarico della tecnologia alla base di Gnutella, ma è anche contestata da molti utenti come un tradimento all'idea di rete originale.



SHAREAZA

VERSIONE CORRENTE: 2.1
RILASCIATA: settembre 2004
INDIRIZZO DI DOWNLOAD: www.shareaza.com/?id=download
DIMENSIONE FILE: 3,56 MB
HOMEPAGE: www.shareaza.com/
NOTE: Supporta Gnutella2, Edonkey 2000 e BitTorrent.

Downloaded File	Size	Progress
Shareaza_2.0.0..	2.50 MB	
192.168.0.231	156 KB	
192.168.0.241	156 KB	
192.168.254.255	156 KB	



LIMEWIRE

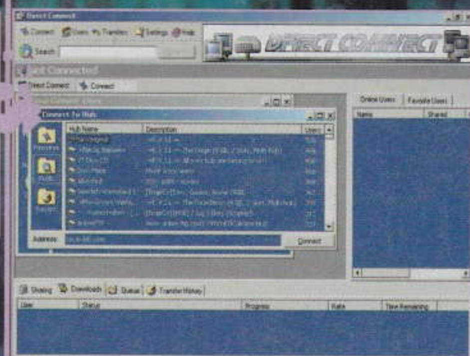
VERSIONE CORRENTE: 4.0.8
RILASCIATA: settembre 2004
INDIRIZZO DI DOWNLOAD: http://www.download.com/LimeWire-International-/3000-2166-10132964.html?part=dl-limewire&subj=dl_int&tag=button
DIMENSIONE FILE: 14,42 MB
HOMEPAGE: http://www.limewire.com/

DIRECTCONNECT

È una delle reti più antiche, è molto simile alla defunta OpenNap di Napster, ma ha la particolarità di selezionare l'accesso concedendolo solo a chi è in grado di mettere in comune file per almeno 3 gigabyte. Questo porta a una selezione naturale che scoraggia chi possiede una connessione lenta. Infatti gli utenti sono solamente circa 400 mila, ma i file sono spesso selezionati e su alcuni hub anche specifici (solo immagini, solo musica, solo filmati, eccetera). Com'era Napster è una rete centralizzata e questo la espone agli attacchi di chi vuole indagare e approfondire ciò che ci scorre sopra. Come nell'agosto di quest'anno, in cui cinque computer collegati a DirectConnect sono stati presi di mira dall'FBI.

DIRECTCONNECT

VERSIONE CORRENTE: 2.2.05
RILASCIATA: marzo 2004
INDIRIZZO DI DOWNLOAD:
www.neo-modus.com/weeklies/DCWeekly.exe
DIMENSIONE FILE: 885 KB
HOMEPAGE: www.neo-modus.com



DC++

VERSIONE CORRENTE: 0.4034
RILASCIATA: marzo 2004
INDIRIZZO DI DOWNLOAD:
http://prdownloads.sourceforge.net/dcplusplus/DCPlusPlus-0.4034.exe?download
DIMENSIONE FILE: 2322 KB
HOMEPAGE:
http://dcplusplus.sourceforge.net/
NOTE: è l'alternativa OpenSource a DirectConnect



SoulSeek

È una rete per chi non si accontenta delle tonnellate di MP3 che può trovare su tutte le altre. Se stiamo cercando musica elettronica, techno o dance, oppure un pezzo che abbiamo ascoltato solamente in locale di New York il sabato sera, qui probabilmente riusciamo a trovarlo.
Più si sponsorizza con piccole donazioni e più si sale nella priorità di download.

SOULSEEK

VERSIONE CORRENTE: 152
RILASCIATA: ottobre 2003
INDIRIZZO DI DOWNLOAD:
www.slsknet.org/slsk152.exe
DIMENSIONE FILE: 738 KB
HOMEPAGE: www.slsknet.org



this script tests if the slsk server is up.

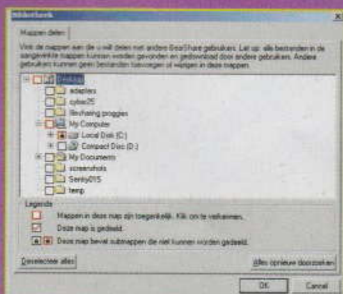
Slsknet.org :: Soulseek Board

probing server... success.

the server is up and running!

BEARSHARE

VERSIONE CORRENTE: 4.6
RILASCIATA: giugno 2004
INDIRIZZO DI DOWNLOAD:
http://download.bearshare.com/BSINSTALLIT.exe
DIMENSIONE FILE: 3,12 MB
HOMEPAGE: www.bearshare.com
NOTE: Ad-ware client!



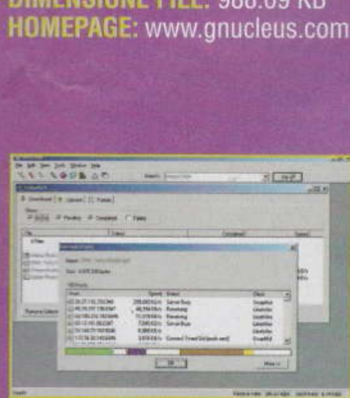


MORPHEUS

VERSIONE CORRENTE: 4.6
RILASCIATA: novembre 2004
INDIRIZZO DI DOWNLOAD:
http://www.download.com/Morpheus/3000-2166-10057840.html?part=dl-morpheus&subj=dl&tag=www
DIMENSIONE FILE: 90 KB
HOMEPAGE:
www.morpheus.com
NOTE: Ad-ware client!

GNUCLEUS

VERSIONE CORRENTE: 4.6
RILASCIATA: novembre 2004
INDIRIZZO DI DOWNLOAD:
http://gnucleus.com/betagnuc/index.php
DIMENSIONE FILE: 988.09 KB
HOMEPAGE: www.gnucleus.com





XOLOX

VERSIONE CORRENTE: 2.0
RILASCIATA: maggio 2004
INDIRIZZO DI DOWNLOAD:
http://www.download.com/3000-2166-10063575.html
DIMENSIONE FILE: 79 KB
HOMEPAGE: http://www.xolox.nl/

METTERE MANO A PHP

Di per sé il file php.ini funziona benissimo così com'è. Ciascuno di noi però ha le sue preferenze, conosce i suoi trucchi e ci tiene a sistemare le cose secondo i suoi gusti. Anche per lavorare più veloci. In un passato numero di Hacker Journal abbiamo già avuto modo di guardare sotto il cofano di php.ini e di modificare parecchi parametri, ma le possibilità sono ancora tante. Vediamo se riusciamo a scovare qualche altro trucco utile.

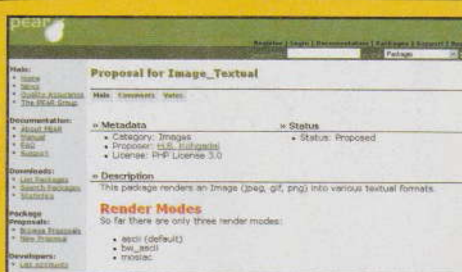
I percorsi migliori

Una variabile del file php.ini è chiamata include_path e serve per impostare dei percorsi di ricerca. Un po' come se caricassimo il sistema di navigazione satellitare con delle mappe per un paese sconosciuto. Diamo al sistema una serie di "dritte" da cui partire per scovare quanto gli serve durante il funzionamento. Poi, se non trova la strada giusta, comunque ce la chiederà, ma prima avrà fatto tutti i tentativi tra quelle che conosce. E che gli abbiamo detto in precedenza con include_path, appunto. Così, quando php avrà a che fare con dei riferimenti a dei file senza una specifica path, un percorso, prima di tutto controllerà nelle directory che gli abbiamo indicato.

Se, per esempio, abbiamo una serie di classi o di librerie che usiamo di frequente, con include_path possiamo elencarne i percorsi per trovarle senza rallentamenti in qualunque momento.
Un altro trucco utile: è anche il posto giusto per specificare le classi PEAR (Php Extension and Application Repository) di php, che ci danno sempre tante

Ognuno di noi ha le sue preferenze.
Nel file php.ini c'è tutto quello che ci serve per farlo funzionare a nostra misura!

Nel progetto Pear si trovano tanti progetti interessanti, come questo per trasformare file .jpeg, .gif, .png in immagini Ascii...



possibilità di scrivere codice pulito e standardizzato. Ecco come scrivere una cosa del genere:

```
include_path=
".:/usr/local/lib/php/pear:"
```

Attenzione utenti Windows: possiamo specificare diverse posizioni separandole dal punto e virgola, a differenza degli utenti Unix che dovranno utilizzare i due punti.

Due variabili sorelle

Auto_prepend_file e auto_append_file sono altre due variabili che possono venire utili in queste occasioni. La prima ci serve per attaccare all'inizio di qualunque documento generato da php un'intestazione. La seconda per attaccare un piè di pagina.

Naturalmente sono molto utili per identificare bene con i nostri dati qualunque documento stiamo generando, senza essere costretti ogni volta a dover aggiungere delle righe di codice.



Sono interessanti soprattutto quando stiamo progettando un server dedicato a una singola applicazione, perché per contro i dati sono aggiunti prima e dopo tutti i documenti che generiamo e questo potrebbe essere inutile o addirittura fastidioso.

Il codice lo possiamo scrivere come uno script php semplice e indipendente, o inglobato in codice Html, naturalmente racchiudendolo tra i tag <?php...?>:

```
auto_prepend_file =
/home/web/includes/header.php
auto_append_file =
/home/web/includes/footer.php
```

Gestire le stupidaggini

Gli errori che possono capitare quando si gestisce php sono più o meno di quattro tipi. Il primo è quello che gli anglosassoni chiamano "fata error" e che non ha bisogno di tante spiegazioni. Quando accade è troppo tardi e generalmente l'applicazione va in stop: si blocca e bisogna mettere mano al codice.

Gli errori non fatali, o avvertimenti, così come gli errori di codice – come una variabile non inizializzata – e gli errori di parsing – quando un'istruzione non viene interpretata – sono le altre possibilità d'errore che php ci segnala con degli appositi avvisi.

Possiamo fare in modo che questi avvisi non ci vengano fatti vedere, ma siano scritti su un file di log che potremo con calma studiare dopo aver testato l'applicazione. Molto interessante soprattutto nella fase di sviluppo. Come si fa? Catturiamo i codici d'errore con la variabile:

```
error_reporting = E_ALL
```

ed evitiamo di farli apparire mettendo a off la variabile

```
display_errors= off
```

Specificare la path è come guardare la mappa del nostro navigatore: trovare la strada sarà molto più semplice.

Infine è bene e utile che li catturiamo in un file di log, che può essere specificato con il valore syslog o con un nome a piacere, in cui raccoglieremo le segnalazioni di errore eventualmente generate. Riassumendo possiamo scrivere così:

```
display_errors = Off
log_errors = On
error_log = "error.log"
```

Sarà poi necessario che andiamo regolarmente a leggere il file error.log, per tenere d'occhio cosa sta succedendo alla nostra applicazione.

ControlBus
controlbus@softhome.net

FARSI UNA PEAR

Pear è un deposito di estensioni e di applicazioni per php che comprende:

- **una libreria** strutturata di codice opensource per utilizzatori di php;
- **un sistema di distribuzione** del codice di manutenzione delle applicazioni;
- **uno stile standard** per la scrittura di codice php;
- **le classi fondamentali** di php;
- **alcune librerie di estensioni;**
- **un sito web,** una mailing list e dei mirror per sostenere la comunità di sviluppatori php

Il sito di riferimento per il progetto Pear è http://pear.php.net/



IL SERVER

È LUI, SULLA FOTO CHE MOSTRA SUL SUO SITO. CHISSÀ DOVE, IN QUALCHE POSTO DELLA ROMANIA !



- Tu hai fatto COSA?!

- ...ma, si, volevamo far accedere all'applicativo direttamente i nostri clienti tedeschi, così dato che di Linux ci capisco un po', ho attribuito al server un IP pubblico e l'ho messo collegato al router, così quelli possono accedere a web server.

- Ma bravo, fortuna che ne capisci di Linux! Quella macchina non era progettata per andare su Internet, non è stata blindata, tutti i servizi sono ora a disposizione del primo script kiddie che passa! A proposito perché mi hai telefonato?

- err, beh un quarto d'ora dopo che ho collegato il server a Internet mi si è bloccato tutto, il gestionale non funzionava più, l'accesso alle pagine web era inibito e non si vedevano più le stampanti. Ho provato a entrare colla telnet ma mi dà accesso negato con qualsiasi utente. Allora ho spento tutto, ma non potendo entrare per fare lo shutdown ho staccato l'interruttore. Ora mi dice di dare la password di root per poter controllare i dischi, ma la password non funziona.

- Complimenti, hai battuto tutti i record di vulnerabilità. Non oso immaginare cosa può esserci dentro quel server. Naturalmente, hai le copie di tutto aggiornate a ieri sera, vero?!

- Uh... ma intanto come faccio a rimettere in pista il mio server?

- Scordatelo, è stato sicuramente compromesso. Facciamo così, prendi quella macchina e vieni qua, vediamo che cosa si può fare. Naturalmente questo esula dal normale contratto di assistenza, e verrà fatturato a ore.

Due ore dopo, mi ritrovo Dave nel mio laboratorio, a mani vuote.

- Beh? Dov'è la macchina?

- Giù nel parcheggio.

- E perché non l'hai portata su?

- Eh? Ma mi hai detto di prendere la macchina e venire qui, io non ho portato nulla!

- Ossignur...la macchina!, il server!, il computer!, non la macchina automobile! Ora riprendi la tua automobile, torna da dove sei venuto, e carica la macchina in macchina cioè il computer dentro l'automobile!



Linux sotto i ferri

Il giorno dopo riesco ad avere in laboratorio il disastrato server.

- Ok, siediti, che così vedi anche tu che disastro hai combinato.

Dato che non si riesce a entrare neanche da console con la password di root, lo attivo in modalità single user mode: reboot ... init... boot: linux S e comincio l'ispezione.

"Mmh strano, sotto la /usr/bin non vedo anomalie, anche con ps non vedo processi anomali, però passwd non funzia. Probabilmente hanno installato un rootkit".

Installo il mio fido chkrootkit (www.chkrootkit.org) per verificare.

...typpette clickete tip tap aahh! ecco qua! il vandalo ha installato il famigerato Romanian rootkit.

Forte, guarda! Ha sostituito tutti i comandi fondamentali: ps, login, netstat, anche l'ls; tutte le directory che si chiamano RK come rootkit sono invisibili! Clickete








Ogni riferimento a fatti e persone non è per nulla casuale. *L'unico indirizzo che non esiste più è quello di Roli: l'hanno chiuso. Forse...*

clack... Guarda, il file /var/log/messages non è stato pulito: riesco a vedere l'ora e il momento in cui il tizio è entrato, e... guarda qui! il log di FTP! Il quaglione si è connesso al suo sito e ha scaricato il suo rootkit, poi ha iniziato a compilarlo e installarlo, poi qualcosa è andato stor-

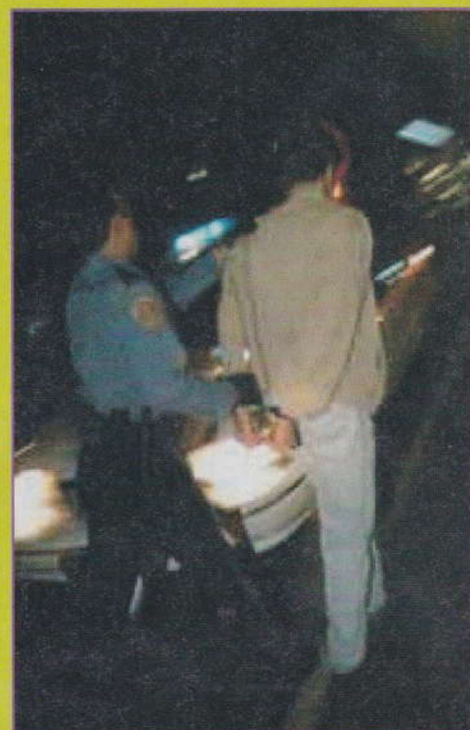


to e non è riuscito più a connettersi, visto che ha sputtanato il programma di login. Ma ora io ho l'indirizzo del suo covo! Quasi quasi gli faccio una visita...
Ecco qua: http://roli.3x.ro... un rumeno! Una volta erano i bulgari i kattivi... bene bene, vediamo che cosa abbiamo qui. Che gente, neanche una password per tappare il suo sito, proprio un pivello
Documents
Virus
Hacks
Passwords
CreditCards
urka!
Vediamo CreditCards... guarda qua che lista di numeri!
Posto pericoloso, questo...
Vediamo Virus: winuke.exe, fbi.exe... bella collezione, fortuna che qui ci sono solo macchine Linux e OSX!
Vediamo Documents: logs, shells, passwords di root e questo che è? Commands? Ma guarda, il manuale dei comandi MS Dos! Ah! Altro che tosto, questo non sa nemmeno i comandi Dos! E' un kiddie dell'ultima ora, però si è impegnato, tutti quei numeri di CC... E qui, guarda, è pure vanitoso, c'è la sua foto! Andiamo oltre, ma forse non mi conviene perdere tempo così... 'spetta, un bel colpo di wget -a -r http://roli.3x.ro/home/gonzo (www.gnu.org/software/wget/wget. html) e mi succhio tutto :-D
Vediamo, abbiamo anche l'accesso ftp in scrittura?
ftp **ftp@roli.3x.ro**
password **roli**
entrato!
quasi quasi gli cancello tutto... no, forse e meglio agire in un altro modo: faccio una visita anche al sito della Polizia(www.poliziadistato.it/pds/informatica/contatti.html) e segnalo questo covo di ladri: uno che raccoglie password e numeri di carte di credito non è altro, anche se tutti i suoi programmi di cracking li tiene in una directory chiamata Hacks. Certo che non so se la polizia italiana potrà fare qualcosa contro un malfattore che sta in Romania, ma lo comunicheranno alle autorità competenti. Io il mio dovere di onesto hacker l'ho fatto.
Mmmh, qui ci sono dei virus, potrebbe essere pericoloso lasciare questa roba in giro, ora tarro tutto e crypto: tar cvf gonzo.tar /home/gonzo;
gpg -e Rick gonzo.tgz (www.gnupg.org)

E ora piallo questo cadavere di macchina; dove sono i CD di Linux? Ah eccoli qua, via! Ok, adesso che il server è rinato e quello sciamannato del tuo capo lo vuole mettere in Internet, gli do una patchata (che parola orribile): installo l'ultima di OpenSSL (www.openssl.org) in inetd.conf, attivo telnet solo per gli indirizzi locali, quindi spengo tutti i servizi che non servono. Speriamo che il nostro abbia veramente le copie di backup aggiornate, altrimenti qualcuno (ke non sono io!) dovrà stare in ufficio, sabato e domenica...

Riccardo Ghiglianovich

FINTI INNOCENTI

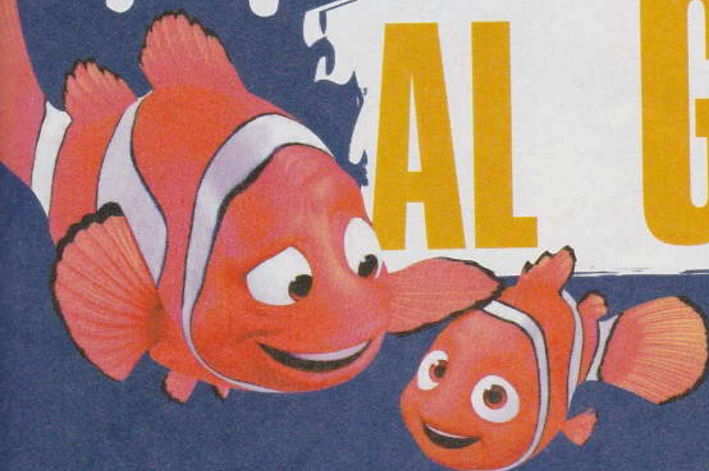


UNO CHE RACCOGLIE PASSWORD E NUMERI DI CARTE DI CREDITO *È UN LADRO,* ANCHE SE TUTTI I SUOI PROGRAMMI DI CRACKING LI TIENE IN UNA DIRECTORY CHIAMATA HACKS



"Segnalare fattacci non vuole dire fare le spie, **ma contribuire a dare dell'hacker la giusta immagine."**

TWOFISH AL GIORNO...



...levan gli intrusi di torno!

Quando la crittografia è solida, non c'è aggressore che tenga. Un algoritmo da raccomandare

Twofish è un cifrario a blocchi realizzato dai Counterpane Labs ed è stato uno dei cinque finalisti candidati a costituire l'Advanced Encryption Standard (AES). Twofish è bello perché libero da brevetti, privo di copyright e license free, libero per tutti gli utilizzi. Ecco perché potrebbe essere una scelta ideale per le nostre attività di programmazione dove serve una cifratura potente e affidabile. Tecnicamente parlando, stando alla descrizione che ne dà l'autore Bruce Schneier, Twofish è un cifrario a blocchi a 128 bit che accetta chiavi di lunghezza variabile, fino a 256 bit. L'algoritmo è implementabile anche direttamente nell'hardware, usando un totale di 14 mila porte logiche.

La cifratura avviene in sedici round nei quali accade veramente di tutto tra trasformazioni, rotazioni, calcoli matriciali, inversioni, funzioni varie e manipolazione delle chiavi. La progettazione di round e avvicendamento delle chiavi fa sì che sia possibile utilizzare l'algoritmo anche dovendo scegliere il migliore compromesso tra velocità, dimensioni del software, tempo di generazione delle chiavi e memoria a disposizione.

L'algoritmo è relativamente vecchio, essendo nato nel 1998. Tuttavia ancora oggi rimane estremamente sicuro: gli attacchi crittanalitici condotti contro Twofish sono arrivati al massimo a smontare cinque round su sedici, il che vuol dire che per arrivare alla sua sconfitta completa ci vorrà ancora un bel po'. In compenso la sua affidabilità è ipercollaudata, tanto che lo usano numerosissimi programmi tra cui anche GNU Privacy Guard (GnuPG), la versione open source di PGP. Una descrizione completa di Twofish (quasi impossibile da fare bene in due paginette!) si trova nel Pdf all'indirizzo http://www.schneier.com/paper-twofish-paper.pdf. Il fatto che Twofish sia anzianotto semplifica le cose anche rispetto al suo utilizzo. Nel tempo si sono rese disponibili librerie un po' per tutti i linguaggi più praticati: C, Delphi, Java, Optimized C, Perl e anche Visual Basic. Inoltre, per le implementazioni in assembly e direttamente nell'hardware, sono disponibili quelle per Pentium e per processori ancora molto usati in applicazioni specifiche, come Z80 e 6805. Per iniziare una ricerca di librerie e implementazioni si può partire dalla pagina http://www.schnei er.com/twofish-download.html, ma in Rete si trova ancora altro: per esempio a http://sourceforge.net/projects/twofish-py/ si trova il progetto versione Python di Twofish.

Si parlerà ancora di Twofish su Hacker Journal. Per quanto l'algoritmo sia vecchiotto, è tuttora molto robusto e relativamente facile da utilizzare nei nostri programmi. Per chi volesse provare a utilizzarlo ci racconti come va a finire ed eventualmente ci mandi il proprio eseguibile, o il codice, o ambedue: lo pubblicheremo nel CD-ROM di Hackers Magazine!

Kurt Gödel
kurtgoedel@hackerjournal.it



Twofish è tuttora tra gli algoritmi di cifratura usati da GnuPG.

"Il papà di Twofish, Bruce Schneier"

RSA Conference 2003

SULLA CARTA DI IDENTITÀ

NOME: *Twofish*

PROFESSIONE: *algoritmo di cifratura a blocchi*

BLOCCHI: *da 128 bit*

CHIAVI: *da 128, 192 o 256 bit*

ROUND: *16*

VELOCITÀ: *18 clock per byte su un Pentium, 16,1 clock per byte su Pentium Pro*

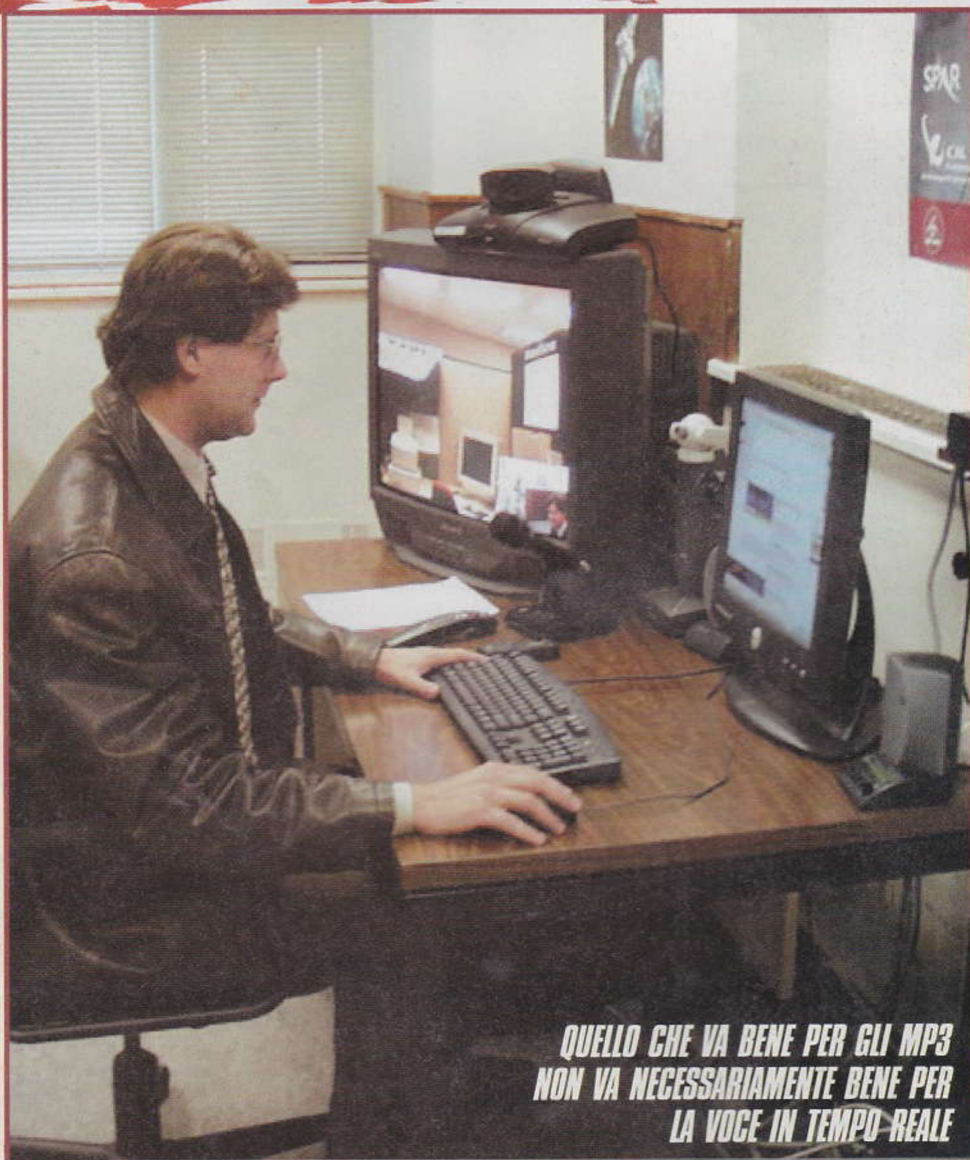
SEGNI PARTICOLARI: *setup efficiente delle chiavi su grossi microprocessori, efficiente su smart card, efficiente se implementato in hardware, già sottoposto a crittanalisi intensa, non brevettato, senza copyright, libero e gratuito.*

ALZA LA VOCE

Come configurare le schede hardware per fare viaggiare la voce su Internet senza pagare il pizzo a Telecom

Ma a che serve una scheda per fare Voice over IP e inviare la voce su Internet per audiochat e telefonate? Serve, serve. La scheda audio normale, che troviamo sul nostro computer di casa, può non essere ottimizzata per trattare la voce. Per fare bene VoIP il sonoro va compresso e decompresso molto rapidamente, secondo protocolli specifici. Quello che va bene per gli MP3 non va necessariamente bene per la voce in tempo reale. La prima scheda che prendiamo in esame è la Phonejack di Quicknet. È una scheda audio normale, ISA o PCI, ma in più possiede l'accelerazione VoIP. Supporta protocolli come G.711, normale e mu/A-law, G.728, G.729, TrueSpeech (G.723.1) e LPC10. Incorpora un connettore telefonico (così possiamo chiamare dal telefono) e anche gli ingressi per microfono e diffusori. La scheda può funzionare senza un IRQ. In Windows la si installa con il suo driver e richiede il programma Internet Switchboard. L'uno e l'altro si prelevano dal sito Quicknet, http://www.quicknet.net.

In Linux invece, oltre al driver giusto, bisogna per forza usare un programma open source come openphone oppure ohphone. Si trovano all'indirizzo http://www.openh323.org/code.html. Openphone e ohphone esistono anche per Windows e costituiscono alternative possibili a Internet Switchboard. Sia su Windows che su Linux i programmatori hanno a disposizione un Software Development Kit, reperibile a



QUELLO CHE VA BENE PER GLI MP3 NON VA NECESSARIAMENTE BENE PER LA VOCE IN TEMPO REALE

IN RETE

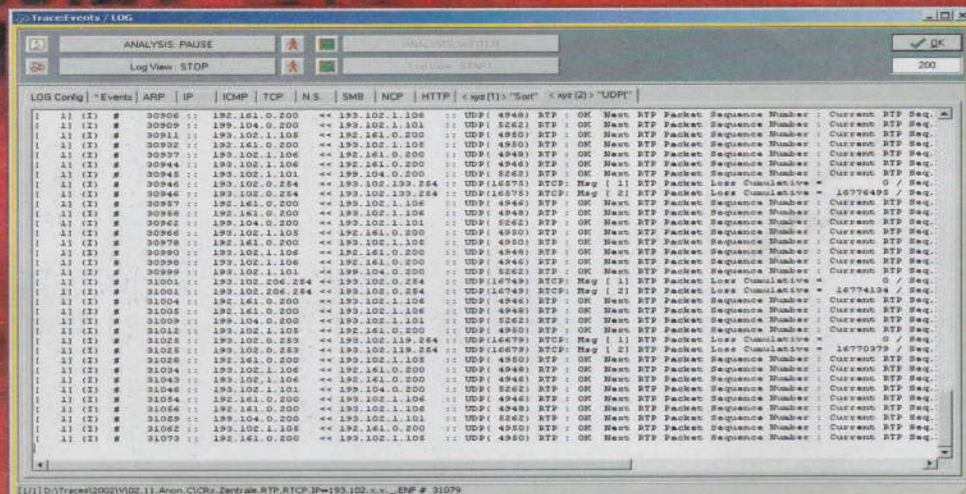
PROGRAMMI CHE USANO H.323

Microsoft NetMeeting - http://www.microsoft.com/windows/netmeeting/
Net2Phone - http://www.net2phone.com/
DialPad - http://www.dialpad.com/
Software open source (per esempio GnomeMeeting e Ohphone nell'ambito del progetto OpenH323 - http://www.openh323.org/

SWITCHBOARD IN AZIONE

Nel sollevare la cornetta, Internet Switchboard entra in azione e attende che digitiamo il numero da chiamare. Possiamo digitare un asterisco e poi comporre un numero IP, mettendo asterischi al posto dei punti, e terminando con #. Oppure si compone un normale numero di telefono, dove occorre sempre il prefisso di chiamata internazionale (per l'Italia è 0039). Per chiamare in VoIP un numero normale occorre essere registrati presso un gateway a cui pagheremo il costo della chiamata.Siccome Internet Switchboard è compatibile H.323, possiamo anche chiamare un computer dove risponde qualcuno munito di NetMeeting. I programmi free di openh323, come openphone o ohphone, possono comunque sostituire Internet Switchboard.

ftp://ftp.quicknet.net/Developer/Linux/Docs/. Con un po' di lavoro in più in fase di compilazione del codice, tutto il software open source dovrebbe funzionare anche su Mac OS X. A volte è già pronto da scaricare, come a http://xmeeting.sourceforge.net/ o http://www.ioxperts.com/apps_osXvideo.html.



▲ ***Se si perdono pacchetti per strada, la trasmissione della voce naufraga. La voce packet loss è la più temuta dagli amministratori di rete.***

La differenza di LineJack

Un'altra scheda di Quicknet, LineJack, fornisce opzioni molto simili a quelle di LineJack e, in più, funziona anche come gateway. In un ipotetico server VoIP la LineJack permetterebbe lo smistamento delle chiamate tra computer in rete. A questo scopo è però necessario scaricare il software MicroTelcoGateway, che si trova a http://www.quicknet.net/download/index.htm. In un prossimo articolo affronteremo il setup concreto di reti VoIP, prima molto semplici e poi progressivamente sempre più complicate.

Nyarlathotep

INSTALLARE SU N-GAGE

Il parco giochi del nostro cellulare preferito può crescere con facilità. Ecco come!





In giro per la Rete si trova un sacco di giochi in formato .blz, che apparentemente non possono funzionare sul nostro Nokia N-Gage. Ma non è esattamente così. Ecco le istruzioni per installare su N-Gage tutti i giochi che vogliamo! Dove parliamo di collegamento tra N-Gage e PC, parliamo di collegamento Bluetooth. Se per qualche motivo non è possibile, il collegamento via cavetto USB funziona ugualmente. Per il resto non c'è problema.

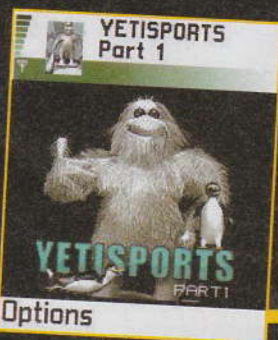
Step one: avere un file .blz

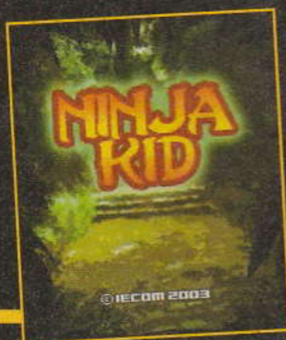
Su Internet i giochi sono tutti compressi in qualche modo e i file avranno estensione tipo .zip, .rar, .ace, .iso o altro. Usiamo WinACE (http://www.winace.com/) per scompattarli. Se il formato è .iso, il programma giusto è IsoBuster (http://www.smart-projects.net/isobuster/). Intanto scarichiamo il programma b_l_z.sis da http://users.skynet.be/FunkyG/N-Gage/Games/b_l_z.sis.

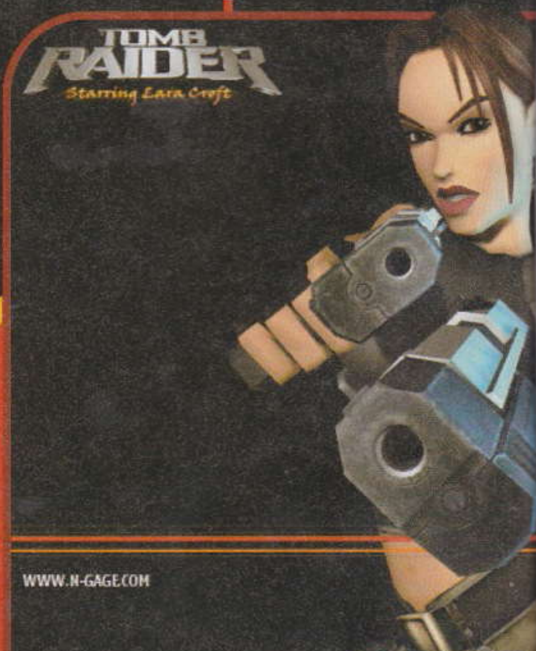
Step two: installare il file .sis

Dopo avere collegato il cellulare al PC, trasferiamo il file .sis nella directory principale della scheda di memoria installata nel cellulare stesso e scolleghiamo. Premiamo il il tasto MENU, apriamo la cartella TOOLS e apriamo MANAGER. Apparirà un elenco dei file .sis installati. Selezioniamo b_l_z e premiamo il tasto di selezione a sinistra così da selezionare











GIOCHI .BLZ N-GAGE



Una nuova icona. Serve a installare i giochi

OPTIONS. Scorriamo e tra le opzioni apparirà Install. Selezioniamola e ripremiamo il tasto di selezione. Vedremo il messaggio Installation security warning. Unable to verify supplier. Continue anyway? e selezioniamo YES (certo che vogliamo installare!). Un altro messaggio chiederà Install b_l_z? e ancora una volta la risposta sarà YES. Dobbiamo ancora selezionare Install e dare l'OK. Il cellulare chiederà dove vogliamo installare. Scorriamo in basso fino a selezionare M. card. Usciamo dalla procedura con il tasto di selezione a destra.

Step three: la parte più facile

Nell'elenco delle icone dovrebbe ora apparirne una nuova, con il nome di blzinstapp. A questo punto abbiamo inserito in N-Gage un installatore di giochi in formato .blz. Per trasferire i giochi veri e propri colleghiamo PC e cellulare e trasferiamo i file .blz nella directory di root della scheda di memoria, proprio come si è fatto prima. Scolleghiamo e apriamo blzinstapp.

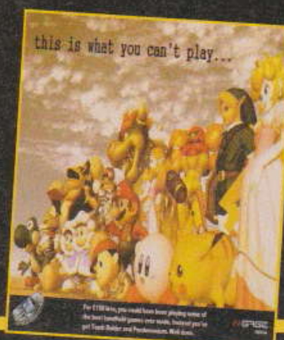
Ci troveremo dentro il gioco. Clicchiamolo con il tasto di selezione ed esso inizierà a installarsi. È importante non interrompere la procedura in questo momento e lasciare che finisca.

Al termine, il file .blz verrà cancellato automaticamente dalla scheda di memoria e il gioco comparirà regolarmente nell'elenco del tasto MENU.

È tutto. Divertiamoci!

Reed Wright
reedwright@mail.inet.it

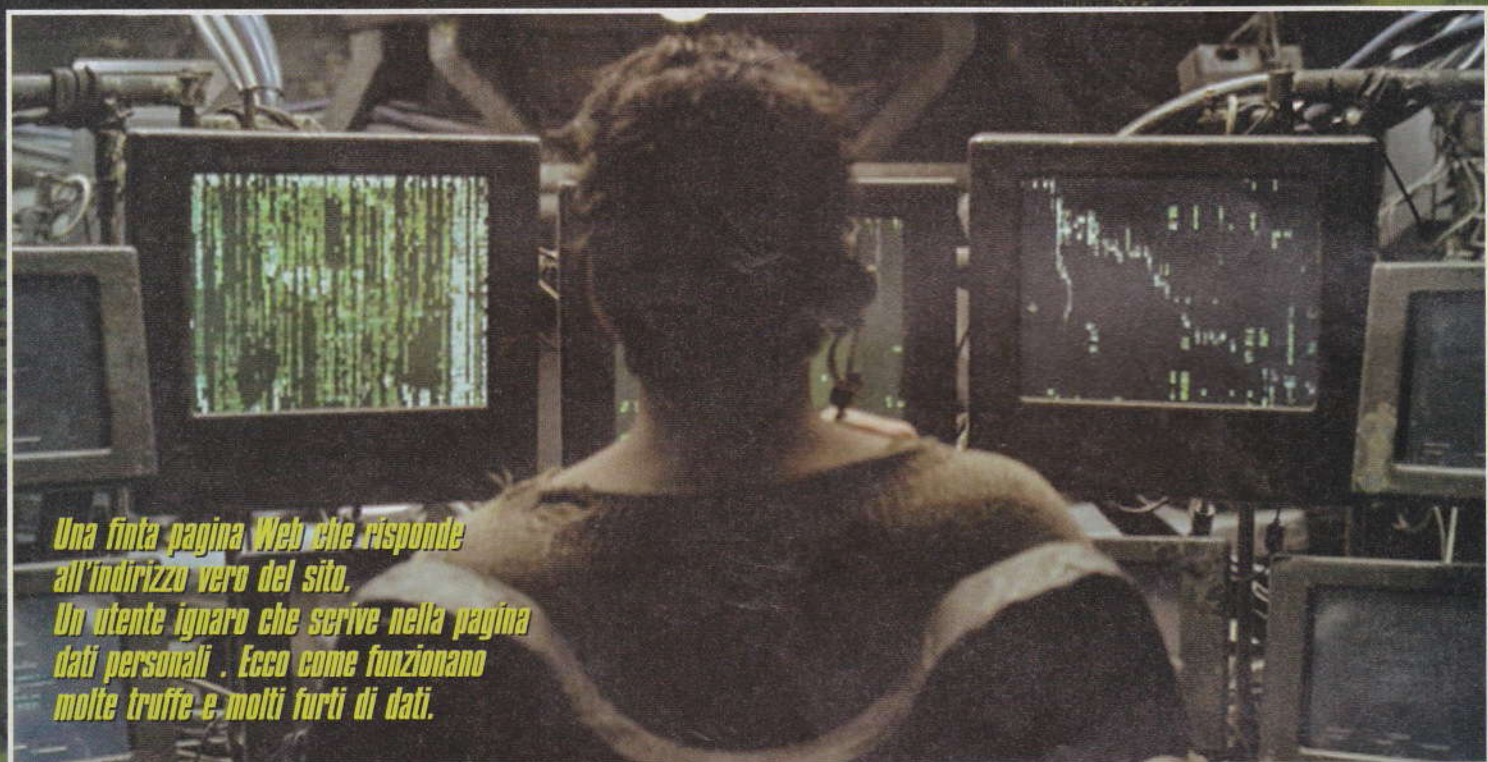






DNS POISONING E DOMAIN

Far credere al mondo che un sito è stato defacciato deviando le richieste dei browser a un altro...



Una finta pagina Web che risponde all'indirizzo vero del sito. Un utente ignaro che scrive nella pagina dati personali . Ecco come funzionano molte truffe e molti furti di dati.

Controinformazione, disinformazione, terrorismo. Crediamo di leggere una notizia su un certo sito e invece stiamo leggendo qualche altra cosa, da qualche altra parte, e qualcuno ha deviato il cammino del nostro browser senza che questo sia subito evidente. Le tattiche per arrivare a questo risultato sono due: DNS poisoning (o DNS spoofing) e domain hijacking. Il primo significa avvelenamento del DNS e consiste nel convincere un name server che un certo dominio ha un indirizzo IP diverso da quello normale. Il secondo significa dirottamento di DNS ed è un vero e proprio furto di dominio. È passata alla storia la "violazione" del sito di RSA nel 2000. E sì che RSA si occupa di sicurezza, hanno pensato molti! Ma il sito non è stato mai violato. Piuttosto, il falsificatore di DNS che ha realizzato l'impresa ha creato un sito che sembrava quello di RSA e poi ha introdotto informazioni alterate nel name server ("avvelenando" la cache di quest'ultimo: da qui il vocabolo poisoning, in modo che l'URL del sito RSA puntasse, erroneamente, alla pagina finta. Quando il visitatore vedeva la finta pagina home alterata, supponeva che fosse stato violato il sito.

La maggior parte dei siti sul Web è vulnerabile a un attacco di questo tipo, che è piuttosto semplice e non tocca il server Web del sito, che può essere protetto quanto si vuole. Tanto non conta; l'attacco non lo sfiora neanche.

La chiave dello spoofing

Quando scriviamo http://www.hackerjournal.it, in realtà scriviamo, senza saperlo, 212.66.104.65. Ricordare l'indirizzo numerico sarebbe un problema, quindi è stato pensato un sistema che traduce da nome "umano" a numero senza che noi dobbiamo faticare. Chiaramente, se qualcuno cambia la tabella di traduzione, sono guai.

L'attacco tipico in questa situazione consiste nell'alterare il cosiddetto record del dominio, conservato presso Network Solutions per i siti .com, presso il NIC per



...sito, che sembra quello originale e defacciato? Si può. Ecco come

HIJACKING

Caro utente, stiamo installando software più sicuro. Ti dispiace reinserire i tuoi dati, così che questa finta pagina PayPal si metta in tasca le tue informazioni di carta di credito?

i siti .it e vari altri registrar. All'indirizzo http://www.securiteam.com/securitynews/Domain_Hijacking__A_step-by-step_guide.html è presente una guida dettagliata su come sferrare un attacco a un sito di esempio.

Come proteggersi

Per prevenire questo tipo di attacco è necessario che la sicurezza sia nel sistema di gestione dei DNS. Se per esempio un gestore di domini accetta via email cambiamenti alle informazioni sul dominio, la mail dovrebbe viaggiare cifrata e autenticata via PGP, oppure dovrebbe esserci a disposizione una pagina Web sicura per effettuare i cambiamenti. Una delle soluzioni migliori emerse finora è DNSSEC, o DNS Security. Questo sistema combina crittografia a chiave pubblica con firma digitale per autenticare chiunque chieda informazioni su un dominio. Dopotutto una mail falsa si mette insieme in pochi istanti. Inoltre valgono sempre le solite raccomandazioni. Una password debole è meno protettiva, meglio una password robusta; controllare regolarmente con WHOIS che i dati relativi ai propri domini siano a posto; guardare le statistiche di accesso e vedere se c'è qualcosa di strano, per esempio un crollo di visite improvviso e senza ragione.
Un DNS poisoning non causa danni veri e propri e quindi, se non si sta attenti, il rischio è che nemmeno ce ne accorgiamo. Intanto la gente va su un'altra pagina...

Beth
i5b3773r@mac.com

I CONSIGLI DI NEO

PER CAPIRE E APPROFONDIRE

DNS: Domain Name System, sistema dei nomi di dominio. I nomi dei domini esistono in forma numerica (come 17.112.152.32: a chi corrisponde?), ma per facilitarci le cose si è creato un meccanismo che li traduce in nomi comuni (come www.linux.org: qual è la sua forma numerica? La corrispondenza tra nomi e numeri figura in database che stanno presso chi vende domini e poi in una serie di server sparsi per Internet. Quando il browser chiede un sito, viene rinviato a un server che gli dà il DNS corretto. I server (DNS server) vengono periodicamente aggiornati con i cambiamenti di informazione. Se le informazioni sono errate, al nome giusto corrisponde un numero sbagliato. Network Solutions: http://www.netsol.com. Il più vecchio e rinomato gestore di nomi di dominio americani e internazionali.
NIC: http://www.nic.it. Il gestore italiano dei nomi di dominio



FRODI DI CARTA

Tra ingegneria sociale e software ostile, ecco i pericoli che corre la nostra carta di credito. Un solo dato certo: sono di più le truffe "nel mondo reale" che quelle on-line

Il tipo più comune di frode sulle carte di credito è quello, nessuno ci crederà, dei possessori! Un sacco di gente falsifica i dati al momento della compilazione dei documenti oppure si dà da fare per farsi alzare i limiti di spesa. L'obiettivo? Riuscire a spendere soldi che non si hanno veramente. A volte c'è un intento chiaro di frodare, a volte invece si tratta solo di persone incapaci di gestirsi.

La frode in questo caso è particolare, ai danni non di un'utente ma di una banca. Esaminando i moduli di richiesta di una carta si scopre che non è così difficile fornire storie e dati personali inventati. Il ladro spende, raggiunge il limite di spesa appena può e, al momento di ricevere il conto, non si farà trovare (l'indirizzo sarà inventato o di altri, chiaro). Per ovvi motivi questa frode non funziona sulle prepagate (o carte di debito).

Sempre sullo stesso registro esiste il kiting, la tecnica di pagare la carta di credito con... un'altra carta di credito. È una tecnica che funziona solo per breve tempo e occasio-



Pagare per abbonarsi a un sito porno è sempre una delusione. Alla fine ci si annoia e quelli non smettono più di addebitare la carta!

nalmente. Come in una catena di Sant'Antonio, entro breve il cerchio magico si spezza. Molti possessori di carta cercano di contestare gli acquisti. Se un acquisto viene contestato e risulta effettivamente non autorizzato dal proprietario, quest'ultimo viene rimborsato. Difficile, però, che si possa fare a lungo. Un esempio tipico è il prelievo di denaro da un Bancomat via carta di credito (non serve la firma!), prelievo che poi viene contestato dicendo che non è mai avvenuto. Notizia per gli sprovveduti: sempre più spesso i Bancomat sono sorvegliati da telecamere. A volte la telecamera è nascosta dentro il Bancomat! Alla contestazione del prelievo, la banca mostra il filmato dello stesso e il trucco muore.Ora cambiamo prospettiva e parliamo di frodi condotte da chi una carta ce l'ha, ma di un altro però.

Le frodi degli altri

Il modo più semplice per attaccare una carta di credito è recuperarne una. Come si può immaginare esiste un ricco mercato nero. Una delle frodi tipiche è quella del buon samaritano. Ci rubano il portafogli o la borsetta e, mannaggia, anche la carta di credito. Un'ora dopo telefona qualcuno. "Ho trovato il suo portafogli… i soldi sono spariti, ma carta di credito e patente ci sono ancora. Purtroppo sto partendo proprio ora per un viaggio di lavoro, ma torno tra tre giorni e le riporto tutto, tanto passo vicino a lì per andare in ufficio". Poteva andare peggio? No, è già peggio. Chi ci casca non va a denunciare il furto e attende i tre giorni per riavere carta e patente. Nel frattempo il ladro si scatena e prosciuga la carta fino all'ultimo centesimo. Soluzione? Offrirsi subito di andare a ritirare il portafogli di persona. Se a chiamare è un ladro, farà resistenza, e con- ►

PORNOTRUFFE

Aldo ogni tanto sbircia in un sito proibito. Un giorno si è lasciato tentare e con la carta di credito ha pagato un abbonamento veramente da poco, tipo cinque dollari al mese, a un sito pornografico. Si è accorto presto che non vale la pena di spendere soldi su cose del genere e, vinto dalla noia, ha disdetto l'abbonamento. Dopo un po' però si è accorto che il sito faceva finta di niente e continuava ad addebitargli sul conto i famosi cinque dollari ogni mese.



Aldo non si è perso d'animo: ha subito allertato la società emettitrice della carta e sono cominciati gli accertamenti. Solo che il sito, apparentemente americano, faceva capo a una società-fantasma residente in un paradiso fiscale sperduto nel Pacifico e non si trovava un responsabile vero.
Aldo ha tenuto duro e alla fine ce l'ha fatta, ma ci sono voluti alcuni mesi. Ovviamente non era questione di soldi (cinque dollari non sono neanche quattro euro), ma di principio, e questo è il trucco dei siti porno. Tantissima gente ci casca e, un po' per pigrizia un po' per vergogna, sopporta e si rassegna al prelievo mensile. Ecco come fanno soldi i siti porno.



verrà denunciare immediatamente il furto. C'è caso che entro tre giorni arrivi sì la carta, ma quella nuova.

Altre categorie di vittime: sbadati. Quelli che si dimenticano di firmare la carta, e ci pensa il ladro al posto loro. Sfigati. Quelli che gli rubano la carta e il ladro capita in negozi dove la firma neanche la guardano. Nella carta di credito, la firma è tutto. Talmente tutto che deve bastare per l'acquisto. Quando la cassiera chiede il codice postale o un documento (in molti ipermercati succede), è giusto rifiutare gentilmente e se necessario chiedere di parlare con un responsabile. Se la carta di credito non sta in una lista nera, deve essere accettata e punto. La firma andrebbe quindi sempre verificata e disgraziatamente numerosi negozianti non lo fanno. In un prossimo numero approfondiremo ulteriormente il tema. Nel frattempo, attenzione alle truffe… e ai truffatori.

NeOkOn
neOkOn@hackerjournal.it

LA TRUFFA DELLA PIZZA

Com'è maleducato questo signore, che siamo in coda alla cassa per pagare la pizza con la carta di credito, e sta attaccato, e spinge… forse non è maleducato. Forse è un ladro. Aspetta che tiriamo fuori la carta per memorizzare nome, numero e scadenza intanto che paghiamo. Poi va su Internet e si mette a comprare roba. Difficile? Mica tanto. Si può, si può. Per le persone oneste, che non useranno le conoscenze accumulate, è un bell'esercizio per allenare la velocità di memorizzazione. Come difendersi? Esporre la carta il meno possibile, farsela dare dalla cassiera annoiata che ci si fa vento, appoggiarla sul bancone a testa in giù, che al massimo si veda la firma.



I CESTINI DELLA MERENDA

Un buon hacker conosce l'arte del dumpster diving: frugare nella spazzatura alla ricerca di informazioni. La conoscono anche i ladri di carte di credito. Non possiamo fare niente per i cassetti dei negozi, dove i negozianti conservano gli scontrini senza prudenza alcuna. Per quanto ci riguarda, invece, sempre distruggere gli scontrini. Contengono informazioni sufficienti a causare problemi. La spazzatura nel cestino può essere merenda appetitosa per un ladro.

ENCICLOPEDIA dell'Hacking



È UNA TECNICA DI ATTACCO IN CUI SI PROVANO TUTTE LE POSSIBILI COMBINAZIONI FINO A TROVARE QUELLA GIUSTA, OVVERO QUELLA CHE DÀ ACCESSO AL SISTEMA SOTTO TIRO.
È UTILIZZATA TIPICAMENTE QUANDO CI SI RIFERISCE ALLA CIFRATURA CON UNA CHIAVE SCONOSCIUTA. LO SCOPO È QUELLO DI TROVARE LA CHIAVE GIUSTA. OPPURE QUANDO SI VOGLIA SCOPRIRE UNA PASSWORD.

ESEMPIO

Qualche malintenzionato vorrebbe conoscere il PIN del nostro bancomat. Essendo formato da quattro cifre, ci sono solamente 10 mila possibili combinazioni da provare, da 0000 a 9999, tra cui ovviamente c'è sicuramente quella giusta. Armandosi di pazienza il nostro malintenzionato potrebbe provarle tutte, digitandole sulla tastiera. In realtà, proprio per evitare gli attacchi brute-force, al terzo tentativo fallito la banca impedisce di provarne altri e, addirittura, ritira automaticamente la tessera che potrà essere recuperata solamente dal proprietario.
Spesso il termine brute-force è utilizzato con il significato di "il metodo più rozzo e difficile". Perché nell'esempio del PIN abbiamo considerato solamente quattro cifre, ma in pratica, per una cifratura adeguata, si possono usare per esempio chiavi a 128 bit, le cui combinazioni sono talmente tante che provarle tutte è una bella impresa.
Viceversa l'attaccante potrebbe prima applicare un po' d'intelligenza e cercar di capire se esistono modi più eleganti e facili di risolvere il problema. Una password sconosciuta, per esempio, potrebbe essere costruita sulla base del nome del proprietario, o seguendo logiche più o meno nascoste. Scoperta la logica, l'attacco brute-force è automaticamente ridotto solamente a una piccola parte di combinazioni possibili.

Requisiti

Un attacco brute-force è l'ultima risorsa e quindi il primo requisito è l'intuito, la logica e l'intelligenza. Dopo, e solamente dopo, se proprio l'attaccante non ha strumenti migliori può affidarsi ai programmi che tentano tutte le combinazioni possibili di una data stringa numerica, alfabetica o alfanumerica. Un esempio? Advanced Archive Password Recovery è un programma che riesce quasi sempre a recuperare le password di archivi compressi come .zip, .rar e altri.

Security

Prima di tutto usare sempre password di almeno otto caratteri, completamente casuali, che contengano sia lettere che numeri, sia maiuscole che minuscole, ma anche simboli. O affidarsi a un generatore di password casuali.
In rete sono recuperabili dei software di sicurezza per proteggere i login al server e alla root di diversi sistemi. Limitare anche il numero di tentativi possibili prima che il sistema si rifiuti di proseguire o in modo tale da lasciare passare del tempo prima di poter effettuare un altro tentativo. Facendo perdere tempo all'attaccante è più probabile che si rivolga altrove. Nei sistemi di crittografia usare quelli a gettone sempre variabile.

LINK

Un generatore di password casuali:
http://www.accusolve.biz/mpwgen.html

Uno strumento per il brute force attack ad archivi compessi di cui si è dimenticata la password:
http://www.crackpassword.com/products/prs/integpack/archive/
(funziona con archivi: ZIP (PKZip, WinZip), ARJ/WinARJ, RAR/WinRAR e ACE/WinACE (1.x))

Biometria



RICONOSCIMENTO DI UNA PERSONA ATTRAVERSO ALCUNE CARATTERISTICHE FISICHE. È IL CASO DELLE IMPRONTE DIGITALI, CHE SONO SPECIFICHE PER CIASCUNO DI NOI E QUINDI PERMETTONO DI RICONOSCERCI.

NOI STESSI UTILIZZIAMO QUOTIDIANAMENTE DEI METODI DI RICONOSCIMENTO BIOMETRICO: PER ESEMPIO GUARDANDOCI IN FACCIA GLI UNI CON GLI ALTRI, O ASCOLTANDO IL TIMBRO DELLA VOCE AL TELEFONO.

ESEMPIO

La biometria può riguardare parecchi aspetti della nostra persona. Tra i metodi di autenticazione utilizzati ci sono:
il riconoscimento dell'iride, del palmo della mano, delle impronte digitali, della geometria della mano, della scrittura, della firma manuale, della voce, dell'odore, delle caratteristiche facciali, del DNA.
La biometria quindi è basata su chi realmente siamo, non su ciò che possediamo (come la chiave dell'automobile, la carta di credito ecc.) e nemmeno su ciò che conosciamo (come una password, un PIN, ecc.)
Alcune caratteristiche biometriche sono più sicure di altre. La firma, la scrittura, il timbro della voce, sono tutte caratteristiche che variano con il tempo o con le condizioni ambientali. Le impronte digitali sono più persistenti, salvo incidenti che ne alterino la qualità
L'impronta dell'iride dell'occhio è molto promettente e uno dei metodi più sicuri.



Requisiti

Si possono sperimentare dei sistemi di riconoscimento anche sul proprio pc.
Alparysoft VideoLock funziona sotto Windows e richiede una semplice webcam. Se il volto non è riconosciuto, non si ha accesso al sistema.

Security

La biometria ha ancora molti passi da fare prima di essere considerata una tecnica di riconoscimento sicura. Il riconoscimento del DNA è ormai accettato, ma non così i sistemi di riconoscimento automatico delle impronte digitali. Se le applicazioni non sono critiche, com può essere l'accesso al nostro pc, i sistemi in commercio sono ottimi. Negli aeroporti e negli altri ambienti ad alta protezione stanno comparendo invece sistemi di riconoscimento facciale sofisticati, o apparecchi di riconoscimento dell'iride.

LINK
Alparysoft VideoLock lo possiamo scaricare da:
www.alparysoft.com/prod/videolock/index.php

Qui possiamo scaricare software di riconoscimento delle impronte digitali e programmi di riconoscimento facciale:
www.neurotechnologija.com/download.html

BUON RUNEDÌ: LE RISPOSTE

IL CYBERENIGMA A BASE DI ALFABETI ESOTICI È PIACIUTO! ECCO COME È ANDATA

L'enigma era scritto in perfetto italiano, ma con alfabeti runici. Le frasi erano le seguenti:

PER UMANI: dove si possono trovare sul Web questi font?
PER NANI: come si chiama questo alfabeto? Che razza lo usa nel Signore degli Anelli?
PER ELFI: come si chiama questo alfabeto? Che razza lo usa nel Signore degli Anelli? Conosci un sito che insegni a scrivere con questo alfabeto?
PER PORTATORI DELL'UNICO ANELLO: come si chiama questo alfabeto? Sai ripetere l'iscrizione che stava sull'anello? Sai come è stata resa in italiano?

La frase per umani era, beh, scritta in chiaro. Il font si chiama Ringbearer e si trova a http://simplythe-

anello, diceva come si chiama questo alfabeto? Sai ripetere l'iscrizione che stava sull'anello? Sai come è stata resa in italiano? L'alfabeto è sempre Tengwar. L'iscrizione originale (questa era difficile!) recita ash nazg durbatulûk, ash nazg gimbatul, ash nazg thrakatulûk agh burzumishi krimpatul. In italiano è un anello per domarli, un anello per trovarli, un anello per ghermirli e nel buio incatenarli.
Tutti i font sono gratuiti e si usano tranquillamente su Windows, Linux e Mac OS X.

Le risposte!

PRIMO ARRIVATO: Gemini Nero!
E poi: BufferOverflow (15 anni, auguri!), Pippo Pizza, []Alex[], devilangel666, -._.·¯¯·._.-´(EaglE)`-._.·¯¯·._.-, DarkLink,

ALTRI SITI CONSIGLIATI

Da Gemini Nero
http://eldalie.it/download/Download_Fonts.htm - font
http://www.gis.net/~dansmith/fonts/index.html - font
http://hem.passagen.se/mansb/at/ - font
http://www.limes.com.pl/~miszka/ - font
http://xoomer.virgilio.it/_XOOM/dcomas/Ardalambion/qcourse.htm - corso di Quenya
http://xoomer.virgilio.it/dcomas/Ardalambion/indice.htm - sito tolkieniano
http://www.glyphweb.com/arda/s/sauron.html - Tengwar Annatar
Da BufferOverflow
http://www.geocities.com/Heartland/Meadows/2488/pag2.html - alfabeti runici
Da Pippo Pizza
http://www.shadowofthering.net
Da []Alex[]
http://ardalambion.immaginario.net/AT/teng_quenya.htm - corso di Quenya
Da -._.·¯¯·._.-´(EaglE)`-._.·¯¯·._.-
http://www.signoredeglianelli.org/downloads.asp - font
Da DarkLink
http://digilander.libero.it/ilfossodihelm/linguaggi.htm
Da M@rk01
http://www.musicaecomputer.com/fonts/italianorune_-_fantasy0006.htm - font
http://www.geocities.com/TimesSquare/4948/tengwar/ - Tengwar
http://marconi.altervista.org/modit.html - alfabeti runici
Da .:Surf3r:.